EUROPEAN COMMISSION
DG HEALTH AND FOOD SAFETY
DG COMMUNICATIONS NETWORKS, CONTENT AND TECHNOLOGY

eHealth-units

18TH EHEALTH NETWORK 12-13 NOVEMBER 2020, BRUSSELS, BELGIUM

COVER NOTE

10.4 D7.3: Report on Common Security framework for eHealth (Draft proposal for discussion)

1. Issue at stake

Healthcare providers (HCPs) are Operators of Essential Services (OES) and as such are challenged to take appropriate and proportionate technical and organisational security measures to manage risks posed to the security of network and information systems they employ in their operations.

This Cybersecurity Guide has been elaborated within the eHAction WP7 with the aim to provide an orientation to health care organisations and help navigate the different guidance documents that have been delivered by EU-level collaborative expert teams of Member State representatives and ENISA primarily under the 2016 Directive on security of network and information systems (the NIS Directive).

The establishment of WS12 in January 2020 by the NIS Cooperation Group dedicated to healthcare, where the main goal is to exchange and promote best practices based on the experiences of Member States in addressing identification, mitigation and management of cyber risks in the health sector, is likely to render the maintenance of this Guide unnecessary; there is a need to explore a potential handing over this item of concluded work to WS 12 as a meaningful sustainability approach for this guide.

2. Summary

Over the last decade, there has been an increased awareness concerning information security and cybersecurity. In Europe, the General Data Protection Regulation, the 'NIS Directive' (security of network and information systems) and the Cybersecurity Act, reinforcing the role of ENISA (the EU Agency for Cybersecurity) in orienting the Member States, are the clear political expressions of a new paradigm of encouraging organisations operating inside the EU to rethink their information and IT security management practices. A direct outcome of increased Member State co-operation in addressing the cybersecurity challenge in healthcare has been the publication of a growing volume of guidance, alongside the relevant standards, addressing governments and health and care providers.

This Data and Systems Security Guide (the Guide) is intended to support healthcare providers in designing and implementing information security systems that are capable of protecting the healthcare providers' critical information infrastructure and information resources. This is pursued through supporting them to navigate the available guidance documents that are created collaboratively and maintained at international level. Such decisions are typically shared within the higher management executives in the hospitals responsible for procurement of equipment, ICT systems and related services. Thus, the Guide addresses Chief Executive Officers and Chief Information Security Officers.

However, more management functions may be relevant in European hospitals and as such may also be addressed by this Guide.

It is important, that at this stage, a consultation with the members of WS12 is facilitated, to discuss the potential of this Guide to feed into their prospective work. The Cybersecurity Guide may be then updated to incorporate any potential comments or recommendations of this group and be submitted, together with the outcome of the above consultation, for discussion to the eHealth Network in spring 2021.

3. Format of procedure in the meeting

For written procedure.